Pre-Comment DRAFT

FSA
Security Awareness & Training Framework

July 2003

1.0 INTRODUCTION

FSA employs roughly 1,200 employees, but leverages nearly 8,500 contractors. It is in all parties' interest to have FSA employees and contractors aware of FSA's security objectives, current security practices, and general security knowledge because it better enables them to protect FSA resources.

FSA depends on computer systems to perform its mission, functions and responsibilities. These systems contain a wealth of information and the confidentiality, integrity, and availability of the information on them cannot be properly protected without ensuring that all employees and contractors involved in the development, maintenance, use, and management of these systems:

- Understand FSA's System Security Policy, procedures, and practices;
- Understand their roles and responsibilities related to FSA's mission; and
- Have at least an adequate knowledge of the various management, operational, and technical controls required and available to protect the FSA systems for which they are responsible.

A robust and FSA-wide security awareness and training program is paramount to ensuring that both employees and contractors understand their IT security responsibilities, and properly use and protect the IT resources entrusted to them. FSA's IT security program cannot be fully functional without significant attention given to training both its employees and contractors.

1.1 Purpose

The purpose of this document is to define and document the framework for FSA's Security Awareness and Training programs. This document covers the laws and regulations that require FSA to implement a Security Awareness and training program, the differences between awareness and training, and the topic areas that should be covered for each. The topic areas are consistent with the Department of Education's and FSA's Security Policy. The document does not go beyond suggested topic areas for awareness and training or cover program implementation.

1.2 Policy

Several Federal Documents require FSA to develop and implement security awareness and training. This document supports requirements specified in the Federal Information Security Management Act (FISMA) of 2002 which is found in Title III of The E-Government Act of 2002, Office of Management and Budget (OMB) Circular A-130, Appendix III and the Computer security Act of 1987.

The Federal Information Security Management Act (FISMA) of 2002 tasks the head of each agency with the responsibility to *"ensure that the agency has trained personnel* *sufficient to assist the agency in complying with the requirements [of FISMA] and related policies, procedures, standards and guidelines [.]"* FISMA also requires the head of each agency to *"delegate to the agency Chief Information Officer … (or comparable official …) the authority to ensure compliance with the requirements imposed on the agency, including - … training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities … [.]"*

FISMA also states that the required *"agencywide information security program"* shall include *"security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency of:*

(i) *information security risks associated with their activities; and*
(ii) *their responsibilities in complying with agency policies and procedures designed to reduce these risks[.]"*

Additionally, OMB Circular A-130, Appendix III, addresses training as an element of a system security plan a General Support System (GSS) and also as an element of an application security plan for a Major Application (MA).

Regarding the training element of a system security plan the Circular states,

"Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Such training shall ensure that employees are versed in the rules of the system … and apprise them about available technical assistance and technical security products and techniques. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system."

The Circular states that as part of an application security plan,

"Before allowing individuals access to the application, ensure that all individuals receive specialized training focused on their responsibilities and the application rules. This may be in addition to the training required for access to a system. Such training may very from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high-risk application)."

The Computer Security Act of 1987 also discusses training. It states that, *"Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency"*.

1.3 Definitions

The most significant difference between training and awareness is that training seeks to teach skills that allow a person to perform a specific function, while awareness seeks to focus an individual’s attention on an issue or set of issues. The following definitions describe the relationship between awareness and training in more detail.

1.3.1 Awareness

Security awareness efforts are designed to change behavior or reinforce good security practices. Awareness is defined in National Institute of Standards and Technology (NIST) Special Publication 800-16 as follows: *“Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching a broad audience with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance.”*

1.3.2 Training

Training is defined in NIST Special Publication 800-16 as follows: Training *“strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security (e.g., management, system design and development, acquisition, auditing.”* The skills acquired in training are built upon the awareness foundation.

1.4 Document Structure

In addition to the Introduction, this document contains an “Approach” section divided into two parts:

Awareness topics, and
Training topics.

2.0 APPROACH

As previously stated in the purpose, this document does not go beyond suggesting topics FSA will cover for its security awareness and training program or into the implementation of the program. The topic areas are consistent with the Department of Education’s and FSA’s Security Policy and are derived from guidance provided in NIST Special Publication 800-16 (Information Technology Security Training Requirements) and 800-50 (Building an Information Technology Security Awareness and Training Program). The topic areas were selected in answer to the following questions:

- What behavior does FSA want to reinforce? (awareness); and
- What skill(s) does FSA want the audience to learn and apply?

2.1 Awareness Topics

The goal of awareness is simply to focus attention on good security practices. The message that the awareness effort sends should be short and simple. The message can address one of the topics below, or it can address a number of topics about which FSA employees and contractors should be aware. The awareness audience must include all employees and contractors/sub-contractors at FSA and therefore the topics for awareness should make all individuals aware of their commonly shared IT security responsibilities.

The following is a list of topics for security awareness. They are:

- Password usage – including creation and frequency of changes
- Protection from viruses, worms, Trojan horses, and other malicious code – scanning, updating definitions
- Policy – implications of noncompliance
- Web usage – allowed versus prohibited; monitoring of user activity
- Data backup and storage – centralized or decentralized approach
- Incident response – contact whom? "What do I do?"
- Changes in system environment – increases in risks to systems and data (e.g., water, fire, dust or dirt, physical access)
- Inventory and property transfer – identify responsible organization and user responsibilities
- Personal use and gain issues – systems at work and home
- Personal digital assistant (PDA) security issues – address both physical and wireless security issues
- Use of encryption and the transmission of sensitive/confidential information over the Internet – address agency policy, procedures, and technical contact for assistance
- Laptop security while on travel – address both physical and information security issues
- Personally owned systems and software at work – state whether allowed or not
- Timely application of system patches – part of configuration management
- Software license restriction issues – address when copies are allowed and not allowed
- Supported/allowed software on organization systems – part of configuration management
- Access control issues – address least privilege and separation of duties
- Individual accountability – explain what this means in the organization
- Use of acknowledgement statements – passwords, access to systems and data, personal use and gain
- Visitor control and physical access to spaces – discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity
- Workstation security – discuss use of screensavers, restricting visitors' view of information on screen (preventing/limiting "shoulder surfing"), battery backup devices, allowed access to systems
- Protect information subject to confidentiality concerns – in systems, archived, on backup media, in hardcopy form, and until destroyed

- Email list etiquette – attached files and other rules.

2.2 Training Topics

The message in a training class is catered to a specific audience and should include everything related to security that attendees need to know in order to do their jobs. Training material should be far more in-depth than material used in promoting awareness. The topics listed below answer the question of, "What skill(s) does FSA want its employees and contractors to learn?"

The following table (from NIST 800-16) contains a core set of IT security terms and concepts titled the "ABC's of Information Technology Security." These 26 items are related to the alphabet and are described briefly. It is anticipated that course material developed under this model will build on these terms. The topics covered in FSA security training will also incorporate these 'ABC's."

ABC's of IT Security

A	**A**ssets - Assets are something of value that requires protection. The value of an asset may be monetary or non-monetary. For example, a computer system clearly has a monetary value that may be expressed in terms of its cost of acquisition or replacement. Data, however, is an asset that may have a monetary value (the cost to acquire), a non-monetary value (loss of public confidence regarding data accuracy), or both.
B	**B**ackup - Backup for data and/or processes are critical safeguards in any IT security environment. The concept of backup includes creation and testing of disaster recovery and continuity of operations plans as well as preparation of copies of data files that are stored "out of harm's way."
C	**C**ountermeasures and Controls - Countermeasures, controls, and safeguards are terms that are often used synonymously. They refer to the procedures and techniques used to prevent the occurrence of a security incident, detect when an incident is occurring or has occurred, and provide the capability to respond to or recover from a security incident. A safeguard may be a password for a user identifier, a backup plan that provides for offsite storage of copies of critical files, audit trails that allow association of specific actions to individuals, or any of a number of other technical or procedural techniques. Basically, a safeguard is intended to protect the assets and availability of IT systems.

D	**D**AA and Other Officials - Individuals are responsible for allocating resources. Resources may be allocated to address IT security issues or any of a number of other competing organizational needs. The individual who has such authority for a specific IT system is termed a Designated Accrediting Authority (DAA) or Approving Authority. The individual who has the authority to allocate resources is also responsible for balancing risks and costs and accepting any residual risks in making those decisions. The accrediting authorities are often aided in these decisions by certifying authorities who provide assessments of the technical adequacy of the current security environment and recommendations for resolving deficiencies or weaknesses.
E	**E**thics - the body of rules that governs an individual's behavior. It is a product of that individual's life experiences and forms a basis for deciding what is right and wrong when making decisions. In today's environment, ethics are situational (i.e., an individual's definition of what is right and wrong changes depending on the nature of a particular situation). For example, an individual may believe that it is wrong to break into someone's house, but does not think that it is wrong to break into someone's computer system.
F	**F**irewalls and Separation of Duties - Firewalls and separation of duties have similar structures and complementary objectives: a firewall is a technical safeguard that provides separation between activities, systems, or system components so that a security failure or weakness in one is contained and has no impact on other activities or systems (e.g., enforcing separation of the Internet from a Local Area Network). Separation of duties similarly provides separation, but its objective is to ensure that no single individual (acting alone) can compromise an application. In both cases, procedural and technical safeguards are used to enforce a basic security policy that high risk activities should be segregated from low risk activities and that one person should not be able to compromise a system.
G	**G**oals - The goals of an IT security program can be summarized in three words: *confidentiality* - data must be protected against unauthorized disclosure; *integrity* - IT systems must not permit processes or data to be changed without authorization; and *availability* –authorized access to IT systems must be assured.
H	**H**ackers/Crackers - The term "hacker" was originally coined to apply to individuals who focused on learning all they could about IT, often to the exclusion of many other facets of life (including sleeping and eating). A "cracker" is any individual who uses advanced knowledge of networks or the Internet to compromise network security. Typically, when the traditional hacker compromised the security of an IT system, the objective was academic (i.e., a learning exercise), and any resulting damage or destruction was unintentional. Currently, the term hacker is being more widely used to describe any individual who attempts to compromise the security of an IT system, especially those whose intention is to cause disruption or obtain unauthorized access to data. Hacker/cracker activity generally gets high press coverage even though more mundane security incidents caused by unintentional actions of authorized users tend to cause greater disruption and loss.

I	**I**ndividual Accountability/Responsibility - A basic tenet of IT security is that individuals must be accountable for their actions. If this is not followed and enforced, it is not possible to successfully prosecute those who intentionally damage or disrupt systems, or to train those whose actions have unintended adverse effects. The concept of individual accountability drives the need for many security safeguards such as user identifiers, audit trails, and access authorization rules.
J	**J**ob Description/**J**ob Function - To provide individuals with the training necessary to do their job, and to establish appropriate safeguards to enforce individual accountability, it is necessary to know what functions an individual is authorized to perform (i.e., their role(s) within the organization). Some times this is accomplished using formalized/written job descriptions. In other situations, such assessments are based on analysis of the functions performed.
K	**K**eys to Incident Prevention - Many IT security incidents are preventable if individuals incorporate three basic concepts into their day-to-day activities: one, awareness – individuals should be aware of the value of the assets they use to do their job and the nature of associated threats and vulnerabilities; two, compliance - individuals should comply with established safeguards (e.g., scanning diskettes, changing passwords, performing backups); and three, common sense - if something appears too good to be true, it generally is.
L	**L**aws and Regulations - Congress has enacted a number of laws (e.g., Privacy Act, Computer Security Act, Computer Fraud and Abuse Act) that establish the basic policy structure for IT security in the Federal government. These laws have been augmented with regulations and guidance regarding their applicability to IT systems. Private industry generally grounds its security policies on the impact on profitability and potential risk of lawsuits, as there are few specific legal requirements. The commonality between Federal and private IT security programs demonstrates that the objectives are the same whether the impetus is a law or the bottom line.
M	**M**odel Framework - This document presents a model framework for IT security training. The model framework describes individual training needs relative to job function or role within the organization. The model recognizes that an individual's need for IT security training will change, both in scope and depth, relative to their organizational responsibilities.
N	**N**eed to Know - Need to Know is addressed from two perspectives: first, a need for access to information to do a job; and second, need to know as a driver for continued learning. In the first case, access to information and processes should be restricted to that which the individual requires to do their job. This approach minimizes the potential for unauthorized activities, and maximizes the potential that the individual knows and understands the nature of the threats and vulnerabilities associated with their use or maintenance of an IT system; and second, given the rate of technological change, individuals need to know the characteristics of those technologies so they may be better able to address specific vulnerabilities.

O	**O**wnership - Responsibility for the security of an IT system or asset must be assigned to a single, identifiable entity, and to a single, senior official within that entity. This provides for accountability for security failures and establishment of the chain of command that authorizes access to and use of system assets. This concept of individual responsibility and authority is generally termed ownership or stewardship. The ownership of an asset (particularly data) is generally retained, even when that asset is transferred to another organization. For example, tax data shared with other Federal and state agencies by the Internal Revenue Service must be secured in accordance with the Internal Revenue Code.
P	**P**olicies and **P**rocedures - IT security safeguards are intended to achieve specific control objectives. These objectives are contained within security policies that should be tailored to the needs of each IT system. Procedures define the technical and procedural safeguards that have been implemented to enforce the specified policies. IT security procedures may be documented in a security plan.
Q	**Q**uality Assurance/**Q**uality Control - Quality Assurance and Quality Control are two processes that are used to ensure the consistency and integrity of security safeguards. Specifically, these processes are intended to ensure that security countermeasures perform as specified, under all workload and operating conditions.
R	**R**isk Management - Risk management is the process whereby the threats, vulnerabilities, and potential impacts from security incidents are evaluated against the cost of safeguard implementation. The objective of Risk Management is to ensure that all IT assets are afforded reasonable protection against waste, fraud, abuse, and disruption of operations. Risk Management is growing in importance as the scope of potential threats is growing while available resources are declining.
S	**S**ecurity Training - Security training is the sum of the processes used to impart the body of knowledge associated with IT security to those who use, maintain, develop, or manage IT systems. A well trained staff can often compensate for weak technical and procedural safeguards. Security training has been demonstrated to have the greatest return on investment of any technical or procedural IT security safeguard.
T	**T**hreats - Threats are actions or events (intentional or unintentional) which, if realized, will result in waste, fraud, abuse, or disruption of operations. Threats are always present, and the rate of threat occurrence can not be controlled. IT security safeguards, therefore, must be designed to prevent or minimize any impact on the affected IT system.
U	**U**nique Identifiers - A unique identifier is a code or set of codes that provide a positive association between authorities and actions to individuals. Safeguards must be in place to ensure that an identifier is used only by the individual to whom it is assigned.

V	**V**ulnerabilities - Vulnerabilities are weaknesses in an IT system's security environment. Threats may exploit or act through a vulnerability to adversely affect the IT system. Safeguards are used to mitigate or eliminate vulnerabilities.
W	**W**aste, Fraud, and Abuse - Waste, fraud, and abuse are potential adverse impacts that may result from a breakdown in IT security. Waste, fraud, and abuse are specifically identified as potential impacts in government-wide policy.
X	e**X**pect the une**X**pected - IT security safeguards target unauthorized actions. Unauthorized actions (acts by individuals or Acts-of-God) can take many forms and can occur at any time. Thus, security safeguards should be sufficiently flexible to identify and respond to any activity that deviates from a pre-defined set of acceptable actions.
Y	**Y**ou - You are responsible and will be held accountable for your actions relative to an IT system or its associated data. You can strengthen or weaken an IT security environment by your actions or inactions. For example, you can strengthen an IT environment by changing passwords at appropriate intervals and weaken it by failing to do so.
Z	**Z**oning/Compartmentalization - Zoning/Compartmenting is a concept whereby an application is segmented into independent security environments. A breach of security would require a security failure in two or more zones/compartments before the application is compromised. This layered approach to security can be applied within physical or technical environments associated with an IT system.

The following set of generic topics (also found in NIST 800-16) expand on the basic concepts introduced in the ABC's, are the foundation for IT security training, and provide a mechanism for FSA employees and contractors to relate and apply the information learned to their duties on the job.

Topic 1: Laws and Regulations

Subjects to include:

- Federal IT security laws, regulations, standards and guidelines
- Organization specific policies and procedures
- Role of Federal government-wide and organization specific laws, regulations, policies, guidelines, standards and procedures in protecting the organization's IT resources
    - Tangible and intangible IT resources (assets)
- Current and emerging social issues that can affect IT assets
- Laws and regulations related to social issues affecting security issues
- Effect of social issues on accomplishment of organizations mission(s)
    - Social conflicts with the Freedom of Information Act
    - Public concern for protection of personal information

- Legal and liability issues
    - Laws concerning copyrighted software
    - Organization policies concerning copyrighted software
    - Laws concerning privacy of personal information
    - Organization policies concerning privacy of personal information
    - Mission related laws and regulations
    - Effects of laws, regulations or policies on the selection of security controls

Includes basic IT security concepts introduced in the following ABC's:
L - Laws and Regulations
P - Policies and Procedures

Topic 2: FSA and IT Security

Subjects to include:

- Organization mission(s)
- How information technology supports the mission(s)
- Reliance on IT systems for mission accomplishment
- IT security programs protect against violations of laws and regulations
- Purpose and elements of organizational IT security programs
- Difference between organization level and system level IT security programs
- Changing IT security issues and requirements
- System ownership and its importance from a user or client perspective
- Information ownership and its importance from a user or client perspective
- Identification of IT security program and system level points of contacts

Includes basic IT security concepts introduced in the following ABC's:
A - Assets
G - Goals
O – Ownership

Topic 3: System Interconnection and Information Sharing

Subjects to include:

- Increased vulnerabilities of interconnected systems and shared data
- Responsibilities of system or information owner organizations if systems have external users or clients
- Responsibility of users or clients for notifying system owners of security requirements
- Sharing information on system controls with internal and external users and clients

- Formal agreements between systems for mutual protection of shared data and resources
    - User rules of behavior and individual accountability in interconnected systems
    - System rules of behavior and technical controls based on most stringent protection requirements
- Electronic mail security concerns
- Electronic commerce
    - Electronic Fund Transfer
    - Electronic Data Interchange
    - Digital/electronic signatures
- Monitoring user activities

Includes basic IT security concepts introduced in the following ABC's:
A - Assets
C - Countermeasures and Controls
E - Ethics
H - Hackers/Crackers
I - Individual Accountability/Responsibility
T - Threats
V - Vulnerabilities
W - Waste, Fraud, and Abuse
X - eXpect the uneXpected
Y – You

Topic 4: Sensitivity

Subjects to include:

- Categorization of system sensitivity
    - Criticality
    - Unauthorized use
    - Reliability
- Categorization of information sensitivity
    - Sensitive information in general
        - Types of sensitive information
        - Aggregation of information
    - Organization's sensitive information
        - Need to know
        - Authorized access
        - Unauthorized disclosure
- IT asset protection requirements
- The organization's need for confidentiality of its information
    - Adverse consequences of unauthorized information disclosure
- The organization's need for integrity of its information

    - Corruption of information
        - Accidental
        - Intentional
    - Adverse consequences if public or other users do not trust integrity and reliability of information
- The organization's need for availability of its information and IT systems
    - Adverse consequences of system or information unavailability
    - Public dependence on information
    - Internal or external user's dependence on information

Includes basic IT security concepts introduced in the following ABC's:
G - Goals
N - Need to Know

Topic 3: Risk Management

Subjects to include:

- Managing risk
    - Threats
    - Vulnerabilities
    - Risk
    - Relationships between threats, vulnerabilities, risks
- Threats from "authorized system users"
- Increased threats and vulnerabilities from connection to external systems and networks
    - "Hacker" threats
    - Malicious software programs and virus threats
- Types of security controls (safeguards, countermeasures)
    - Management controls
    - Acquisition/development/installation/implementation controls
    - Operational controls
    - Security awareness and training controls
    - Technical controls
- How different categories of controls work together
- Examples of security controls for:
    - Confidentiality protection
    - Availability protection
    - Integrity protection
- Added security controls for connecting external systems and networks
- Protecting assets through IT security awareness and training programs
- Contingency-disaster recovery planning
    - Importance of plan to deal with unexpected problems
    - Importance of testing plan and applying lessons learned

- “Acceptable levels of risk” vs. “absolute protection from risk”
- “Adequate” and “appropriate” controls
  - Unique protection requirements of IT systems and information
  - Severity, probability, and extent of potential harm
  - Cost effective/cost benefits
  - Reduction of risk vs. elimination of risk
- Working together with other security disciplines
- Importance of internal and external audits, reviews, and evaluations in security decisions

Includes basic IT security concepts introduced in the following ABC’s:
C - Countermeasures and Controls
R - Risk Management
S - Security Training

Topic 6: Management Controls

Subjects to include:

- System/application-specific policies and procedures
- Standard operating procedures
- Personnel security
  - Background investigations/security clearances
  - Roles and responsibilities
  - Separation of duties
  - Role-based access controls
- System rules of behavior contribute to an effective security environment
  - Organization-specific user rules
  - System-specific user rules
    - Assignment and limitation of system privileges
    - Intellectual property/Copyright issues
    - Remote access and work at home issues
    - Official vs. unofficial system use
    - Individual accountability
    - Sanctions or penalties for violations
- Individual accountability contributes to system and information quality
  - Individual acceptance of responsibilities
  - Signed individual accountability agreements
- IT security awareness and training
  - Determining IT security training requirements for individuals
  - Effect of IT security awareness and training programs on personal responsibility and positive behavioral changes
  - “Computer ethics”
  - System-specific user IT security training

- User responsibilities for inappropriate actions of others

Includes basic IT security concepts introduced in the following ABC's:
E- Ethics
I - Individual Accountability/Responsibility
J - Job Description/Job Function
M - Model Framework
P - Policies and Procedures
S - Security Training
Y – You

Topic 7: Acquisition/Development/Installation/Implementation Controls

Subjects to include:

- System life cycle stages and functions
- IT security requirements in system life cycle stages
    - Initiation stage
    - Development stage
    - Test and evaluation stage
    - Implementation stage
    - Operations stage
    - Termination stage
- Formal system security plan for management of a system
    - Identification of system mission, purpose and assets
    - Definition of system protection needs
    - Identification of responsible people
    - Identification of system security controls in-place or planned and milestone dates for implementation of planned controls
- Relationship of configuration and change management programs to IT security goals
- Testing system security controls synergistically and certification
- Senior manager approval (accredit) an IT system for operation

Includes basic IT security concepts introduced in the following ABC's:
D - DAA and Other Officials
G - Goals
O – Ownership

Topic 8: Operational Controls

Subjects to include:

- Physical and environmental protection
    - Physical access controls
    - Intrusion detection
    - Fire/water/moisture/heat/electrical maintenance
    - Mobile and portable systems
- Marking, handling, shipping, storing, cleaning, and clearing
- Contingency planning
    - Importance of developing and testing contingency/disaster recovery plans
    - Importance of users providing accurate information about processing needs, allowable down time and applications that can wait
    - Responsibility for backup copies of data files and software programs
    - Simple user contingency planning steps

Includes basic IT security concepts introduced in the following ABC's:
B - Backup
Z - Zoning/Compartmentalization

Topic 9: Technical Controls

Subjects to include:

- How technical (role-based access) controls support management (security rules) controls
    - User identification and passwords/tokens
    - User role-based access privileges
    - Public access controls
- How system controls can allow positive association of actions to individuals
    - Audit trails
    - System monitoring
- Recognizing attacks by hackers, authorized or unauthorized users
    - Effects of hacker attack on authorized users
    - Unauthorized use or actions by authorized users
    - Incident Response reporting, chain of command
- User actions to prevent damage from malicious software or computer virus attacks
    - Organization specific procedures for reporting virus incidents
    - Technical support and help from security incident response teams
    - Software products to scan, detect and remove computer viruses
- Role of cryptography in protecting information

Includes basic IT security concepts introduced in the following ABC's:
F - Firewalls and Separation of Duties
H - Hackers/Crackers
I - Individual Accountability/Responsibility
J - Job Description/Job Function
K - Keys to Incident Prevention

Q - Quality Assurance/Quality Control
U - Unique Identifiers
V - Vulnerabilities
Z - Zoning/Compartmentalization

3.0 NEXT STEPS

Since this document discusses only the topic areas that should be covered for security training and awareness, FSA now needs to develop the material to cover all these topics and determine;

- Who should be trained,
- What topics are they going to be trained on, and
- How they will be trained.

Once these items are determined FSA can implement an effective security training and awareness program.